



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/635,389	08/06/2003	Wendell M. Smith	01251-P0011B	1191
24126 7590 12/10/2007 ST. ONGE STEWARD JOHNSTON & REENS, LLC 986 BEDFORD STREET STAMFORD, CT 06905-5619			EXAMINER SINGH, SATWANT K	
			ART UNIT 2625	PAPER NUMBER
			MAIL DATE 12/10/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

Response to Amendment

1. This office action is in response to the amendment filed on 12 September 2007.

Response to Arguments

2. Applicant's arguments with respect to claims 1, 15, 21, 26-3030 and 32 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-4, 6, 7, 9, 12, 15-27, and 32 rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik et al. (US 7,031,471) in view of Dresevic et al. (US 6,313,920).
5. Regarding Claim 1, Stefik et al teaches a document security system for printing secured documents comprising: a digital file (digital work) accessible by a receiver via a terminal (external interface for receiving and transmitting data) (col. 5, lines 46-49); a printer connected to the terminal (rendering device) (col. 6, lines 4-13); security data (watermark) specific to each page of said digital file (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7); and a mark printed by said printer on each page of the printed digital file (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7).

Stefik et al fails to teach a mark containing data specific to each page of the printed digital file.

Dresevic et al teaches a mark containing data specific to each page of the printed digital file (identifiers for all of the glyphs in the TextOut call which have not been used on previous pages in the document) (col. 10, lines 1-14).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Dresevic to identify the glyphs/watermarks used in the document to specify data specific to the current page which are different from the glyphs/watermarks on the other pages of the document.

6. Regarding Claim 2, Stefik et al teaches a document security system for printing secured documents wherein said printer is connected to said terminal via a network connection (digital works are distributed from trusted systems to trusted rendering devices via computer networks) (col. 4, lines 58-60).

7. Regarding Claim 3, Stefik et al teaches a document security system for printing secured documents further comprising an identification device for identifying the sender (Fig. 5) (tags "Description" 501, "Work-ID" 502 and "Owner" 503 provide identification information for the digital work) (col. 8, lines 60-65).

8. Regarding Claim 4, Stefik et al teaches a document security system for printing secured documents wherein a second identification device (print right) is provided at the printer wherein the printer will not print (***it is interpreted by the examiner that if the printer repository does not have a print right, it will not decrypt the digital work***)

said digital document unless identification data gathered by the second identification device matches stored identification data (Fig. 4, S406) of users that are allowed access to said digital document (Fig. 4, S407) (if the digital work has the print right, the printer repository decrypts the digital work and generates the watermark that will be printed on the digital work) (col. 7, lines 55-67, col. 8, lines 1-20).

9. Regarding Claim 6, Stefik et al teaches a document security system for printing secured documents wherein the security system encrypts said digital file prior to said digital file being sent to the printer (digital works and various communications are encrypted whenever they are transferred between repositories) (col. 6, lines 1-3).

10. Regarding Claim 7, Stefik et al teaches a document security system for printing secured documents wherein said mark is selected from the group consisting of: a Watermark or an Optical Variable Device (the rendered work is watermarked to record data about the digital work and the rendering event) (col. 5, lines 1-7).

11. Regarding Claim 9, Stefik et al teaches a document security system for printing secured documents wherein the characteristics of said mark are selected from the group consisting of covert data (invisible watermark), overt data (visible watermark) or combinations thereof (multiple watermarking techniques) (col. 8, lines 32-36).

12. Regarding Claim 12, Stefik et al teaches a document security system for printing secured documents further comprising verification data gathered by the security system for verifying whether the sender (repository 1) has clearance access said digital file (Fig. 4, S401) (digital work is assigned usage rights) (col. 7, lines 60-65).

13. Regarding Claim 15, Stefik et al teaches a document security system for printing secured documents comprising: a digital file (digital work) accessible by a sender via a terminal (external interface for receiving and transmitting data) (col. 5, lines 46-49), said digital file comprising at least two pages to be printed (pages of a digital work) (col. 12, lines 15-16); a printer connected to the terminal via a network (rendering device) (col. 6, lines 4-13); security data (watermark) specific to each page of the digital file (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7); and at least two marks (visible and invisible watermarks) (col. 8, lines 30-45) printed by said printer on the at least two pages of the printed digital file (pages of a digital work) (col. 12, lines 15-16), and said at least two marks being different from each other (visible versus invisible) (col. 8, lines 30-45).

Stefik et al fails to teach said marks containing data specific to each of the at least two pages of the printed digital file.

Dresevic et al teaches said marks containing data specific to each of the at least two pages of the printed digital file (identifiers for all of the glyphs in the TextOut call which have not been used on previous pages in the document) (col. 10, lines 1-14).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Dresevic to identify the glyphs/watermarks used in the used in the document to specify data specific to the current page which are different from the glyphs/watermarks on the other pages of the document.

14. Regarding Claim 16, Stefik et al teaches a document security system for printing secured documents further comprising verification data gathered by the security system for verifying whether the sender (repository 1) has clearance access said digital file (Fig. 4, S401) (digital work is assigned usage rights) (col. 7, lines 60-65).

15. Regarding Claim 17, Stefik et al teaches a document security system for printing secured documents wherein said verification data includes identification of the sender (Fig. 5) (tags "Description" 501, "Work-ID" 502 and "Owner" 503 provide identification information for the digital work) (col. 8, lines 60-65).

16. Regarding Claim 18, Stefik et al teaches a document security system for printing secured documents wherein the security system encrypts said digital file prior to said digital file being sent to said printer (digital works and various communications are encrypted whenever they are transferred between repositories) (col. 6, lines 1-3).

17. Regarding Claim 19, Stefik et al teaches a document security system for printing secured documents wherein said mark is a watermark (the rendered work is watermarked to record data about the digital work and the rendering event) (col. 5, lines 1-7).

18. Regarding Claim 20, Stefik et al teaches a document security system for printing secured documents wherein the characteristics of said mark are selected from the group consisting of covert data (invisible watermark), overt data (visible watermark) or combinations thereof (multiple watermarking techniques) (col. 8, lines 32-36).

19. Regarding Claim 21, Stefik et al teaches method for printing secured documents comprising the steps of: collecting verification data from a sender relating to a digital file

(assigned usage rights) (col. 7, lines 55-67, col. 8, lines 1-20); verifying access to the digital file based upon the collected verification data (Fig. 4, S401) (digital work deposited into repository 1) (col. 7, lines 55-67, col. 8, lines 1-20); accessing the digital file (Fig. 4, S402 and S403) (repository 1 transfers a copy of the digital work to repository 2) (col. 7, lines 55-67, col. 8, lines 1-20); inputting a print command (Fig. 4, S404) (repository 2 receives a user request to print the digital work) (col. 7, lines 55-67, col. 8, lines 1-20); generating security data related to the verification data (watermark information to be placed on the digital work associated with the rendering or distribution event) (col. 8, lines 30-44), the security data being specific to each page of the digital file to be printed (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7); encrypting the digital file (digital works and various communications are encrypted whenever they are transferred between repositories) (col. 6, lines 1-3); sending the encrypted digital file to a printer (Fig. 4, S406) (printer repository receives the encrypted digital work) (col. 7, lines 55-67, col. 8, lines 1-20); and printing the digital file with a mark on each page of the document (Fig. 4, S408) (printer generates the watermark that will be printed on the digital work) (col. 7, lines 55-67, col. 8, lines 1-20),.

Stefik et al fails to teach the mark for each page containing data specific to each page of the printed document.

Dresevic et al teaches the mark for each page containing data specific to each page of the printed document (identifiers for all of the glyphs in the TextOut call which have not been used on previous pages in the document) (col. 10, lines 1-14).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Dresevic to identify the glyphs/watermarks used in the used in the document to specify data specific to the current page which are different from the glyphs/watermarks on the other pages of the document.

20. Regarding Claim 22, Stefik et al teaches a method for printing secured documents further comprising the steps of selectively granting the sender (repository 1) access to the digital file based upon the collected verification data (Fig. 4, S401) (digital work is assigned usage rights) (col. 7, lines 60-65).

21. Regarding Claim 23, Stefik et al teaches a method for printing secured documents wherein the verification data includes identification of the sender (Fig. 5) (tags "Description" 501, "Work-ID" 502 and "Owner" 503 provide identification information for the digital work) (col. 8, lines 60-65).

22. Regarding Claim 24, Stefik et al teaches a method for printing secured documents wherein the mark comprises a watermark (the rendered work is watermarked to record data about the digital work and the rendering event) (col. 5, lines 1-7).

23. Regarding Claim 25, Stefik et al teaches a method for printing secured documents wherein the characteristics of the mark are selected from the group consisting of covert data (invisible watermark), overt data (visible watermark) or combinations thereof (multiple watermarking techniques) (col. 8, lines 32-36).

24. Regarding Claim 26, Stefik et al teaches a method for printing secured documents comprising the steps of: accessing the digital file (Fig. 4, S402 and S403) (repository 1 transfers a copy of the digital work to repository 2) (col. 7, lines 55-67, col. 8, lines 1-20); generating security data (watermark) related to the digital file (watermark information to be placed on the digital work associated with the rendering or distribution event) (col. 8, lines 30-44), the security data being specific to each page of the digital file to be printed (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7); sending the digital file to a printer (Fig. 8, S408) (printer repository transmits the decrypted digital file with the watermark to a printer device for printing) (col. 7, lines 55-67, col. 8, lines 1-20); printing the digital file and a mark on each page of the digital file (watermark information placed on the digital work).

Stefik fails to teach the mark containing data specific to each page of the printed digital file.

Dresevic et al teaches the mark containing data specific to each page of the printed digital file (identifiers for all of the glyphs in the TextOut call which have not been used on previous pages in the document) (col. 10, lines 1-14).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Dresevic to identify the glyphs/watermarks used in the used in the document to specify data specific to the current page which are different from the glyphs/watermarks on the other pages of the document.

25. Regarding Claim 27, Stefik et al teaches a document security system for printing secured documents comprising: a digital file (digital work) accessible by a receiver via a computer terminal (external interface for receiving and transmitting data) (col. 5, lines 46-49); security data specific to said digital file (watermark information to be placed on the digital work associated with the rendering or distribution event) (col. 8, lines 30-44) and to each page of said digital file (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7); a printer connected to the computer terminal (rendering device) (col. 6, lines 4-13); and a mark printed by said printer on each page of the printed digital file (watermark information placed on the digital work)

Stefik et al fail to teach said mark containing data specific to each page of the printed digital file.

Dresevic et al teach said mark containing data specific to each page of the printed digital file (identifiers for all of the glyphs in the TextOut call which have not been used on previous pages in the document) (col. 10, lines 1-14).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Dresevic to identify the glyphs/watermarks used in the used in the document to specify data specific to the current page which are different from the glyphs/watermarks on the other pages of the document.

26. Regarding Claim 32, Stefik et al teaches a document security system for printing secured documents comprising: a digital file (digital work) accessible by a sender via a terminal (external interface for receiving and transmitting data) (col. 5, lines 46-49); a

printer connected to the terminal (rendering device) (col. 6, lines 4-13) via a network connection (digital works are distributed from trusted systems to trusted rendering devices via computer networks) (col. 4, lines 58-60); security data specific to each page of said digital file (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7); and a mark printed by said printer (printer repository transmits the decrypted digital file with the watermark to a printer device for printing) (col. 7, lines 55-67, col. 8, lines 1-20) on each page of the printed digital file (watermark information placed on the digital work).

Stefik et al fails to teach said mark containing data specific to each page of the printed digital file.

Dresevic et al teaches said mark containing data specific to each page of the printed digital file (identifiers for all of the glyphs in the TextOut call which have not been used on previous pages in the document) (col. 10, lines 1-14).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Dresevic to identify the glyphs/watermarks used in the used in the document to specify data specific to the current page which are different from the glyphs/watermarks on the other pages of the document.

27. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik et al and Dresevic et al as applied to claim 3 above, and further in view of Carr et al. (US 6,389,151).

28. Regarding Claim 5, Stefik et al and Dresevic et al fail to teach a document security system for printing secured documents wherein said identification device comprises a fingerprint keypad.

Carr et al teaches wherein said identification device comprises a fingerprint keypad (Fig. 3, fingerprint reader 303) (col. 4, lines 63-65).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teaching of Stefik and Dresevic with the teaching of Carr to allow a user to use their fingerprint as identification to print secure documents.

29. Claim 8 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik et al and Dresevic et al as applied to claim 1 above, and further in view of Zorab et al. (US 2003/0177095).

30. Regarding Claim 8, Stefik et al and Dresevic et al fail to teach a document security system for printing secured documents wherein said mark comprises DNA information coded in ink utilized to print said mark.

Zorab et al teaches wherein said mark comprises DNA information coded in ink utilized to print said mark (DNA tag) (page 2, paragraph [0019]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik and Dresevic with the teaching of Zorab to encode one's DNA tag in the watermark information.

31. Regarding Claim 11, Stefik et al and Dresevic et al fail to teach a document security system for printing secured documents wherein said printer uses ink to print

said digital file, said ink selected from the group consisting of: DNA ink or fluorescent ink.

Zorab et al teaches wherein said printer uses ink to print said digital file, said ink selected from the group consisting of: DNA ink or fluorescent ink (fluorescent ink or DNA tag) (page 2, paragraph [0019]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik and Dresevic with the teaching of Zorab to encode the watermark information using a DNA tag or fluorescent ink.

32. Claims 28 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik in view of Dresevic et al and Zorab et al.

33. Regarding Claim 28, Stefik et al teach a document security system for printing secured documents comprising: a digital file (digital work) accessible by a receiver via a computer (external interface for receiving and transmitting data) (col. 5, lines 46-49); a printer connected to the computer (rendering device) (col. 6, lines 4-13); security data specific to said digital file (watermark information to be placed on the digital work associated with the rendering or distribution event) (col. 8, lines 30-44); and a mark printed by said printer with said ink on the printed digital file (watermark information placed on the digital work) (col. 8, lines 30-44) wherein said security data further comprises data specific to each page of said digital file (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7).

Stefik et al fail to teach a document security system for printing secured documents comprising: ink usable by said printer, said ink having coded DNA

information that contains said security data specific to said digital file; and a mark containing data specific the printed digital file.

Zorab et al teaches a document security system for printing secured documents comprising: ink usable by said printer, said ink having coded DNA information that contains said security data specific to said digital file (DNA tag) (page 2, paragraph [0019]).

Dresevic et al teaches a mark containing data specific the printed digital file (identifiers for all of the glyphs in the TextOut call which have not been used on previous pages in the document) (col. 10, lines 1-14).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Dresevic and Zorab to encode one's DNA tag in the watermark information in the glyphs/watermarks used in the used in the document to specify data specific to the current page which re different from the glyphs/watermarks on the other pages of the document.

34. Regarding Claim 30, Stefik et al teach a document security system for printing secured documents comprising: a digital file (digital work) accessible by a receiver via a computer (external interface for receiving and transmitting data) (col. 5, lines 46-49); a printer connected to the computer; security data specific to said digital file (rendering device) (col. 6, lines 4-13); and a watermark printed by said printer on each page of the printed digital file (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44), said watermark containing

data specific the printed digital file (watermark information to be placed on the digital work associated with the rendering or distribution event) (col. 8, lines 30-44) wherein said security data further comprises data specific to each page of said digital file (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7).

Stefik et al fail to teach wherein the watermark is an Optical Variable Device and said Optical Variable Device further contains data specific to each page of said digital file.

Zorab et al teaches wherein the watermark is an Optical Variable Device (optical device such as a hologram or digitally printed device) (page 2, paragraph [0019]).

Dresevic et al teaches an Optical Variable Device further contains data specific to each page of said digital file (identifiers for all of the glyphs in the TextOut call which have not been used on previous pages in the document) (col. 10, lines 1-14).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Zorab to encode the watermark information in the glyphs/watermarks used in the used in the document to specify data specific to the current page which are different from the glyphs/watermarks on the other pages of the document.

35. Claims 10, 13, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik et al and Dresevic et al as applied to claim 1 above, and further in view of Martin et al. US 5,710,420).

36. Regarding Claim 10, Stefik et al and Dresevic et al fail to teach a document security system for printing secured documents wherein said mark is printed on a

medium, said medium selected from the group consisting of: plain paper, paper having a distinct pattern located thereon, or thermal transfer holographic foil.

Martin et al teaches wherein said mark is printed on a medium, said medium selected from the group consisting of: plain paper, paper having a distinct pattern located thereon, or thermal transfer holographic foil (protochromic marking material can be applied to any desired substrate, for example plain papers, ruled papers, bond paper, etc) (col. 8, lines 59-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik and Dresevic with the teaching of Martin to allow a user to embed watermark information on many types of media.

37. Regarding Claim 13, Stefik et al teaches a document security system for printing secured documents wherein said verification data includes identification of the sender (Fig. 5) (tags "Description" 501, "Work-ID" 502 and "Owner" 503 provide identification information for the digital work) (col. 8, lines 60-65).

38. Regarding Claim 14, Stefik et al teaches a document security system for printing secured documents wherein the security system selectively grants the user access to said digital file based upon the collected verification data (print right) (col. 8, lines 9-20).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Satwant K. Singh whose telephone number is (571)

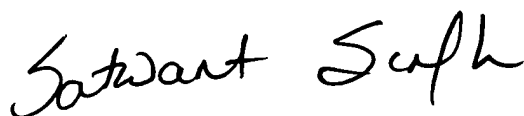
Application/Control Number:
10/635,389
Art Unit: 2625

Page 17

272-7468. The examiner can normally be reached on Monday thru Friday 8am - 4:30pm.

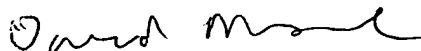
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David K. Moore can be reached on (571) 272-7437. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



sks

Satwant K. Singh
Examiner
Art Unit 2625



DAVID MOORE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600